Theoretical Computer Science 102 (1992) 355–365
Elsevier

Note

An asymptotic equality for the number of necklaces in a shuffle-exchange network*

Lakshman Prasad and S.S. Iyengar

Department of Computer Science, Louisiana State University, Baton Rouge, LA 70803, USA

Communicated by M. Nivat
Received April 1991

Abstract

Prasad, L. and S.S. Iyengar, An asymptotic equality for the number of necklaces in a shuffle-exchange network, Theoretical Computer Science 102 (1992) 355–365.

The search for efficient bounds for VLSI problems has spawned an increasingly important research area. In this paper, we derive an asymptotic equality for the number of necklaces in a shuffle-exchange network, and provide a formula for the number of necklaces of a given length. This symptotic equality for the number of necklaces is an extension to Ullman's result reported in [2].

1. Preliminaries

A shuffle-exchange network with $n=2^k$ nodes has its nodes numbered from 0 to 2^k-1, where each number is expressed in binary. Thus, each node has a k-bit address. The node i is connected to node j if $2i \equiv j \pmod{(2^k-1)}$. (For details see [2].)

Ullman [2] proves that the number of necklaces in a shuffle-exchange of 2^k nodes is $O(2^k/k)$. In this paper, we prove that the number of necklaces in a shuffle-exchange of 2^k nodes is in fact *asymptotically equal to* $2^k/k$.

* This research is partially supported by LEQFS-RD-A-04 Board of Regent's grant and Office of Naval Research N00014-91J-1306.

Lemma 1.1. *If* $2i \equiv j \pmod{(2^k-1)}$ *then the binary representation of* j *is obtained from that of* i *by a left-cyclic shift of one bit.*

Proof. Let $i = a_{k-1}a_{k-2}\ldots a_0$ be the binary representation of i; then

$$i = a_{k-1}2^{k-1} + a_{k-2}2^{k-2} + \cdots + a_0.$$

Therefore,

$$\begin{aligned} 2i &= a_{k-1}2^k + a_{k-2}2^{k-1} + \cdots + a_0 2^1 \\ &= a_{k-1}(2^k - 1) + a_{k-2}2^{k-1} + \cdots + a_0 2^1 + a_k. \end{aligned}$$

Hence,

$$2i \equiv a_{k-2}2^{k-1} + \cdots + a_0 2^1 + a_{k-1} = j \bmod (2^k - 1),$$

i.e.,

$$j = a_{k-2}\ldots a_0 a_{k-1},$$

which is a one-bit left-cyclic rotation of $a_{k-1}a_{k-2}\ldots a_0$. □

2. Structural properties of the shuffle-exchange network

In this section, we look at some structural properties of the shuffle-exchange network useful for deriving the asymptotic equality for the number of necklaces in the network.

Remark 2.1. Every k-bit number comes back to itself after k cyclic shifts.

Remark 2.2. A k-bit number may come back to itself after d cyclic shifts where $d < k$.

Definition 2.3. $i \sim j$ if i differs from j by an r-fold cyclic rotation/shift for some r.

Remark 2.4. "$\sim$" is an equivalence relation.

Definition 2.5. Each equivalence class under the relation $\sim$ is called a *necklace*, and the number of nodes in each necklace is called the *length* of the necklace.

Lemma 2.6. *A shuffle-exchange network of* 2^k *nodes has a necklace of length* d *iff* d *is a factor of* k.

Proof. A node s with a k-bit address $a_1\ldots a_k$ belongs to a necklace of length d iff d is the smallest positive integer such that $a_1\ldots a_k$ is identical to itself shifted cyclically d times, i.e., if $i \equiv j \pmod{d}$ then $a_i = a_j$.

Now let s be a node belonging to a necklace of length d. Let the k-bit address of s be $a_1 \ldots a_k$, and $k = qd + r$, $0 < r < d$.
Thus,

$$s = a_1 \ldots a_k = \underbrace{\overline{a_1 \ldots a_d}\ \overline{a_1 \ldots a_d} \ \ldots\ \overline{a_1 \ldots a_d}\ \overline{a_1 \ldots a_d}}_{q \text{ times}}\ a_1 \ldots a_r.$$

Let

$$a_1 \ldots a_k \rightarrow_t a_{t+1} \ldots a_k a_1 \ldots a_t$$

indicate a t-fold left-cyclic shift of the string.
Then

$$s = \overline{a_1 \ldots a_d} \ \ldots\ \overline{a_1 \ldots a_d}\ a_1 \ldots a_r \rightarrow_d \overline{a_1 \ldots a_d} \ \ldots\ \overline{a_1 \ldots a_d}\ a_1 \ldots a_r a_1 \ldots a_d$$

$$= s'.$$

Since a d-fold left-cyclic shift results in the original string, i.e., $s = s'$, comparing the last d bits of s and s', we have

$$a_1 \ldots a_{d-r} a_{d-r+1} \ldots a_d \equiv a_{r+1} \ldots a_d a_1 \ldots a_r,$$

i.e., these two strings are identical.
That is,

$$A = a_1 \ldots a_{d-r} \equiv a_{r+1} \ldots a_d$$

and

$$B = a_{d-r+1} \ldots a_d \equiv a_1 \ldots a_r.$$

Now

$$AB = a_1 \ldots a_{d-r} a_{d-r+1} \ldots a_d = a_1 \ldots a_r a_{r+1} \ldots a_d = BA.$$

So,

$$s = (AB)^q B.$$

Now

$$s = (AB)^q B = (BA)^q B = BA(BA)^{q-1} B$$

$$\rightarrow_r A(BA)^{q-1} BB = (AB)^q B = s.$$

This implies that s is restored to itself after r left-cyclic shifts. But, $r < d$ and this contradicts the fact that d is the smallest positive number such that $s \rightarrow_d s$.

Hence, $r = 0$ and, therefore, d is a factor of k. □

Remark 2.7. All shuffle-exchanges with necklaces of length d have the same number of necklaces of length d.

Indeed, let one shuffle-exchange have 2^{ld} nodes and the other have 2^{md} nodes. If b is a d-bit string of 0's and 1's which is not made of repetitions of some smaller string, then the string $bb\ldots b$, b repeated l times represents a necklace of length d in the shuffle-exchange of 2^{ld} nodes and the string $bb\ldots b$ repeated m times represents a necklace of length d in the shuffle-exchange of 2^{md} nodes. Thus, there is a one-to-one correspondence between the necklaces of length d of any two shuffle-exchanges having necklaces of length d.

Let $C(d)$ denote the number of necklaces of length d.

Notation. $d \mid k$ denotes that "d is a factor of k" or "d divides k completely."

Lemma 2.8. *The total number of necklaces in a shuffle-exchange of* 2^k *nodes given by* $\sum_{d \mid k} C(d)$ *is asymptotically equal to* $2^k/k$.

Definition 2.9. If $f(x)$ and $g(x)$ are real-valued functions of a real variable x, then $f(x)$ is asymptotically equal to $g(x)$ (written $f(x) \sim g(x)$) if $\lim_{x \to \infty} f(x)/g(x) = 1$.

Thus, the above lemma reads as follows.

2.1. Main lemma

Lemma 2.8.

$$\sum_{d \mid k} C(d) \sim \frac{2^k}{k}.$$

Proof. Note that

(i) every node in a shuffle-exchange belongs to some necklace;
(ii) no two necklaces share the same node;
(iii) a necklace of length d has d nodes in it.

By (i), (ii) and (iii) we have

$$\sum_{d \mid k} dC(d) = 2^k.$$

Now, $d \leqslant k$; so,

$$\sum_{d \mid k} kC(d) \geqslant 2^k,$$

i.e.,

$$\sum_{d \mid k} C(d) \geqslant \frac{2^k}{k}.$$

Therefore,

$$\sum_{d \mid k} C(d) = \Omega\left(\frac{2^k}{k}\right).$$

Now, every node in a necklace of length d has its address obtained by repeated concatenation of a string of length d which itself is not repetitions of a string of smaller length. Thus, $dC(d) \leqslant 2^d$, i.e., $C(d) \leqslant 2^d/d$.
Therefore,

$$\sum_{d|k} kC(d) \leqslant \sum_{d|k} (2^d/d),$$

i.e.,

$$\sum_{d|k} kC(d) \leqslant \frac{2^k}{k} + \sum_{\substack{d|k \\ d<k}} \frac{2^d}{d} = \frac{2^k}{k}\left\{1 + \sum_{\substack{d|k \\ d<k}} \frac{k}{d2^{k-d}}\right\}$$

or

$$\sum_{d|k} kC(d) \leqslant \frac{2^k}{k}\left\{1 + k \sum_{\substack{d|k \\ d<k}} \frac{1}{d2^{k-d}}\right\}.$$

If $d<k$ then $d \leqslant k/2$ for all $k>1$. That is,

$$k - d \geqslant \frac{k}{2}.$$

So,

$$\frac{1}{2^{k-d}} \leqslant \frac{1}{2^{k/2}}.$$

Thus,

$$\sum_{d|k} C(d) \leqslant \frac{2^k}{k}\left\{1 + \frac{kd(k)}{2^{k/2}}\right\},$$

where $d(k)$ is the number of divisors decomposition of k.

If $k>1$ and if $k = p_1^{\alpha_1} p_2^{\alpha_2} \cdots p_m^{\alpha_m}$ then the number of divisors of k,

$$d(k) = (\alpha_1 + 1)(\alpha_2 + 1) \cdots (\alpha_m + 1).$$

Now for all primes p^i and all $\alpha_i \geqslant 0$,

$$p_i^{\alpha_i} \geqslant 2^{\alpha_i} \geqslant \alpha_i + 1.$$

So,

$$k = p_1^{\alpha_1} p_2^{\alpha_2} \cdots p_m^{\alpha_m} \geqslant 2^{\alpha_1} 2^{\alpha_2} \cdots 2^{\alpha_m} \geqslant (\alpha_1 + 1)(\alpha_2 + 1) \cdots (\alpha_m + 1),$$

i.e.,

$$k \geqslant d(k).$$

Therefore,

$$\sum_{d|k} C(d) \leqslant \frac{2^k}{k}\left(1 + \frac{k^2}{2^{k/2}}\right),$$

i.e.,

$$\frac{2^k}{k} \leqslant \sum_{d|k} C(d) \leqslant \frac{2^k}{k}\left(1+\frac{k^2}{2^{k/2}}\right),$$

i.e.,

$$0 \leqslant \left(\frac{\sum_{d|k} C(d)}{\frac{2^k}{k}} - 1 \right) \leqslant \frac{k^2}{2^{k/2}}.$$

So,

$$\lim_{k\to\infty} \frac{\sum_{d|k} C(d)}{2^k/k} = 1,$$

since

$$\lim_{k\to\infty} \frac{k^2}{2^{k/2}} = 0.$$

Hence,

$$\sum_{d|k} C(d) \sim \frac{2^k}{k}. \qquad \square$$

Corollary 2.10. *In particular,*

$$\sum_{d|k} C(d) = \Theta\left[\frac{2^k}{k}\right].$$

3. An exact formula for the number of necklaces of a given length

We now obtain the formula for the number of necklaces of length d. We do this by two interesting methods.

The first method uses the theory of arithmetic functions to obtain a formula, while the second method uses the combinatorial tool of counting known as the "inclusion-exclusion principle."

3.1. First method

3.1.1. Preliminaries

We will introduce some elementary ideas and tools from the theory of arithmetic functions.

Definition 3.1. An arithmetic function f is a mapping from the set of natural numbers $\mathbb{N}$ into the set of complex numbers $\mathbb{C}$.

Remark 3.2. In particular, any function from $\mathbb{N}$ into $\mathbb{N}$ is also an arithmetic function.

3.1.2. Some important arithmetic functions

(i) *Identity function I*:

$$I(n)=\left[\frac{1}{n}\right] \quad \forall n\in\mathbb{N},$$

where $[a]$ is the integer part of any real number a.
That is,

$$I(1)=1,$$

$$I(n)=0 \quad \forall n>1.$$

(ii) *Unit function u*:

$$u(n)=1 \quad \forall n\in\mathbb{N}.$$

(iii) *Möbius function*: If $n=p_1^{\alpha_1}p_2^{\alpha_2}\cdots p_k^{\alpha_k}$ is prime decomposition of a natural number n, then define

$$\mu(1)=1,$$

$$\mu(n)=(-1)^k \quad \text{if } \alpha_1=\alpha_2=\cdots=\alpha_k=1,$$

$$\mu(n)=0 \qquad \text{otherwise.}$$

Remark 3.3. The Möbius function μ of any number divisible by the square of a prime is zero.

Lemma 3.4.

$$\sum_{d\mid n}\mu(d)=I(n).$$

Proof. If $n=p_1^{\alpha_1}p_2^{\alpha_2}\cdots p_k^{\alpha_k}>1$ is the prime decomposition of n, $\alpha_i>0$, $\forall\, 1\leqslant i\leqslant k$, then the only divisors of n for which μ is nonzero are of the form $p_{i_1}\cdots p_{i_r}$, $i_r\neq i_s$, for $r\neq s$, $1\leqslant i_r\leqslant k$ and $1\leqslant r\leqslant k$, and $\mu(p_{i_1}\cdots p_{i_r})=(-1)^r$.

Now, there are ${}^kC_r$ numbers of the form $p_{i_1}\cdots p_{i_r}$, $1\leqslant r\leqslant k$. So,

$$\sum_{d\mid n}\mu(d)=1+\sum_{r=1}^{k}(-1)^r\,{}^kC_r=(1-1)^r=0.$$

If $n=1$ then $\sum_{d\mid n}\mu(d)=\mu(1)=1$. Therefore, $\sum_{d\mid n}\mu(d)=I(n)$. □

3.1.3. Dirichlet convolution of arithmetic functions

Definition 3.5. If f and g are arithmetic functions, their Dirichlet product (denoted as $f*g$) is the arithmetic function defined by

$$(f*g)(n)=\sum_{d\mid n} f(d)g\left(\frac{n}{d}\right).$$

(i) Writing it another way, $(f*g)(n)=\sum_{ab=n} f(a)g(b)$, where it is obvious that $*$ is commutative.

(ii) Since

$$\begin{aligned}[(f*g)*h](n) &= \sum_{ab=n} (f*g)(a)h(b)\\ &= \sum_{ab=n}\sum_{cd=a} f(c)g(d)h(b)\\ &= \sum_{bcd=n} f(c)g(d)h(b)\\ &= \sum_{cm=n} f(c)\sum_{bd=m} g(d)h(b)\\ &= [f*(g*h)](n),\end{aligned}$$

$*$ is associative.

(iii) If f is any arithmetic function and I is the identity function, then

$$(f*I)(n)=\sum_{d\mid n} f(d)I\left(\frac{n}{d}\right)=f(n).$$

So,

$$f*I=f$$

(hence, the name identity function).

(iv) If f and g are arithmetic functions such that

$$f(n)=\sum_{d\mid n} g(d),$$

then

$$f(n)=\sum_{d\mid n} g(d)=\sum_{d\mid n} g(d)u\left(\frac{n}{d}\right)=(g*u)(n),$$

where u is the unit function.

Now

$$\sum_{d\mid n} \mu(d)=I(n).$$

So,

$$\mu*u=I.$$

Thus, μ and u are inverses of each other with respect to Dirichlet convolution.

3.1.4. Möbius inversion formula

If f and g are arithmetic functions such that $f(n)=\sum_{d|n} g(d)\ \forall n\in\mathbb{N}$, then we can "invert" this expression and write g "in terms of" f:

$$f(n)=\sum_{d|n} g(d).$$

We get $f=g*u$. So,

$$f*\mu=(g*u)*\mu=g*(u*\mu)=g*I=g.$$

Therefore, if $f=g*u$, then $g=f*\mu$. That is, if

$$f(n)=\sum_{d|n} g(d),$$

then

$$g(n)=\sum_{d|n} f(d)\,\mu\left(\frac{n}{d}\right) \quad \forall n\in\mathbb{N}.$$

This is called the Möbius inversion formula.

Lemma 3.6.

$$C(d)=\frac{1}{d}\sum_{m|d} 2^m\mu\left(\frac{d}{m}\right).$$

Proof. Since $\sum_{m|d} mC(m)=2^d$, applying the Möbius inversion formula, we have

$$C(d)=\frac{1}{d}\sum_{m|d} 2^m\mu\left(\frac{d}{m}\right). \qquad \square$$

3.2. Second method: the inclusion–exclusion principle

Lemma 3.7. *If $A_1,\ldots,A_n$ are finite sets and $\#(A)$ is the cardinality of the set A, then*

$$\#(A_1\cup\cdots\cup A_n)=\sum_{1\leqslant i\leqslant n}\#(A_i)-\sum_{1\leqslant i<j\leqslant n}\#(A_i\cap A_j)$$
$$+\sum_{1\leqslant i<j<k\leqslant n}\#(A_i\cap A_j\cap A_k)-\cdots+(-1)^n\#(A_1\cap\cdots\cap A_n).$$

Proof. Let $U=\bigcup_{i=1}^n A_i$. For any set A, define the characteristic function of A by

$$\chi_A(x)=\begin{cases}1 & \text{if } x\in A\\ 0 & \text{if } x\notin A\end{cases} \quad \forall x\in U.$$

Thus, $\chi_{A_i}: U\to\{0,1\}$ is the characteristic function of the set A_i.
Clearly,

$$\chi_U(x)=1 \quad \forall x\in U.$$

Also if A^c is the complement set of A, i.e., $A^c = U \setminus A$, then

$$\chi_{A^c}(x) = 1 - \chi_A(x) \quad \forall x \in U$$

and

$$\chi_{A_i \cap A_j}(x) = \chi_{A_i}(x)\chi_{A_j}(x) \quad \forall x \in U.$$

Now

$$\chi_{U^c}(x) = 0 \quad \forall x \in U.$$

Since $U^c = A_1^c \cap \cdots \cap A_n^c$, we have

$$0 = \chi_{A_1^c \cap \cdots \cap A_n^c}(x) = \prod_{i=1}^{n} (1 - \chi_{A_i}(x)) \quad \forall x \in U,$$

i.e.,

$$1 = \sum_{1 \leqslant i \leqslant n} x_{A_i} - \sum_{1 \leqslant i < j \leqslant n} \chi_{A_i}\chi_{A_j} + \cdots + (-1)^n \chi_{A_1}\chi_{A_2}\cdots\chi_{A_n}.$$

Summing the left-hand side and the right-hand side over all elements $x \in U$, we have

$$\sum_{x \in U} 1 = \sum_{x \in U} \sum_{1 \leqslant i \leqslant n} \chi_{A_i} - \sum_{x \in U} \sum_{1 \leqslant i < j \leqslant n} \chi_{A_i}\chi_{A_j} + \cdots + (-1)^n \sum_{x \in U} \chi_{A_1}\chi_{A_2}\cdots\chi_{A_n},$$

and this yields

$$\#(U) = \sum_{1 \leqslant i \leqslant n} \#(A_i) - \sum_{1 \leqslant i < j \leqslant n} \#(A_i \cap A_j) + \sum_{1 \leqslant i < j < k \leqslant n} \#(A_i \cap A_j \cap A_k) - \cdots + (-1)^n \#(A_1 \cap \cdots \cap A_n).$$

Since $\#(U) = \#(A_1 \cup \cdots \cup A_n)$, the result follows. □

This is called the inclusion–exclusion principle. Using this, we shall count the number of necklaces of length d for any positive integer d.

Definition 3.8. If a string of length d is not a concatenation of copies of a smaller string, then it is called a *pure* string of length d, otherwise it is called an *impure* string of length d.

Remark 3.9. Only pure strings of length d contribute to the formation of necklaces of length d.

Let $d = p_1^{\alpha_1} p_2^{\alpha_2} \cdots p_m^{\alpha_m}$ be the prime decomposition of d. Let A_i be the set of all impure strings of length d made of repetitions of strings of length d/p_i or submultiples of it. Then

$$\#(A_i) = 2^{d/p_i}$$

and

$$\#(A_{i_1} \cap \cdots \cap A_{i_r}) = 2^{d/p_{i_1}\cdots p_{i_r}}, \quad 1 \leqslant i_1 < \cdots < i_r \leqslant m, \ 1 \leqslant r \leqslant m.$$

The number of strings of length d is equal to 2^d. The number of pure strings of length d is equal to $2^d - \#(A_1 \cup \cdots \cup A_n)$.

By the inclusion–exclusion principle, we have

$$\#(A_1 \cup \cdots \cup A_n) = \sum_{1 \leqslant i \leqslant n} \#(A_i) - \sum_{1 \leqslant i < j \leqslant n} \#(A_i \cap A_j) + \sum_{1 \leqslant i < j < k \leqslant n} \#(A_i \cap A_j \cap A_k) - \cdots + (-1)^n \#(A_1 \cap \cdots \cap A_n).$$

Therefore, the number of pure strings of length d is given by

$$2^d - \#(A_1 \cup \cdots \cup A_n) = 2^d - \sum_{1 \leqslant i_1 \leqslant n} 2^{d/p_i} + \cdots + (-1)^r \sum_{1 \leqslant i_1 < \cdots < i_r \leqslant n} 2^{d/p_{i_1} \cdots p_{i_r}} + \cdots + (-1)^m 2^{d/p_{i_1} \cdots p_{i_m}}.$$

So,

$$C(d) = \frac{1}{d}\left\{2^d + (-1) \sum_{r=1}^{m} (-1)^r \sum_{1 \leqslant i_1 < \cdots < i_r \leqslant n} 2^{d/p_{i_1} \cdots p_{i_r}}\right\}.$$

Note that this is the same as the formula derived using the Möbius inversion formula, but written without the aid of the Möbius function.

4. Concluding remarks

In this paper, we have presented an *asymptotic equality* for the number of necklaces in a shuffle-exchange network. Also, we present an exact formula for the number of necklaces of a given length using the theory of arithmetic functions and by the inclusion–exclusion principle. This asymptotic equality for the number of necklaces is an extension to Ullman's result reported in [2]. At the time of proof-reading this paper, it was brought to our notice that exact formulae for the number of necklaces in shuffle networks and De Bruijn networks have been obtained by Rowley and Bose [3], also using arithmetic functions, independently. We thank Prof. Bose for his comments on our paper.

References

[1] G. Polya and G. Szego, *Problems and Theorems in Analysis Vols. 1 and 2* (Springer, Berlin, 1972, 1976).

[2] J.D. Ullman, *Computational Aspects of VLSI* (Computer Science Press, 1984) 210–214.

[3] R. Rowley and B. Bose, On necklaces in shuffle exchange and De Bruijn networks, in: *Proc. 1990 Internat. Conf. on Parallel Processing.*